Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - ActiveWeb Active Auction House SQL Injection and Cross-Site Scripting Vulnerability
  - AN HTTP Server 'cmdIS.DLL' Buffer Overflow Arbitrary Code Execution and Cross-Site Scripting Vulnerability
  - Centrinity FirstClass Bookmark Input File Execution Vulnerability
  - Computer Associates eTrust Intrusion Detection Denial of Service Vulnerability
  - DameWare Mini Remote Control Privilege Escalation Vulnerability
  - GNU DC++ Arbitrary Files Modification Vulnerability
  - GNU Maxthon Security ID Disclosure Vulnerability
  - Lightspeed Technologies DeluxeFTP Information Disclosure Vulnerability
  - MailEnable IMAP "LOGIN" Command Buffer Overflow Vulnerability
  - Microsoft Exchange Server Remote Code Execution Vulnerability
  - Microsoft Internet Explorer Remote Code Execution Vulnerability
  - **Microsoft Jet Database Remote Code Execution Vulnerability (Updated)**
  - **Microsoft Media Player & Windows/MSN Messenger PNG Processing (Updated)**
  - Microsoft MSN Messenger Remote Code Execution Vulnerability
  - Microsoft Outlook and Outlook Web Access Email Spoofing Vulnerability
  - **Microsoft Windows ANI File Parsing Errors (Updated)**
  - Microsoft Windows Kernel Elevation of Privilege and Denial of Service Vulnerabilities
  - **Microsoft Windows License Logging Service Buffer Overflow (Updated)**
  - Microsoft Windows Shell Remote Code Execution Vulnerability
  - Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities
  - Microsoft Windows Message Queuing Remote Code Execution Vulnerability
  - Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities
  - Miranda IM PopUp Plus Plugin Remote Code Execution Vulnerability
  - Netscape Browser Information Disclosure Vulnerability
  - Network-Client.com FTP Now Local Information Disclosure Vulnerability
  - Ocean12 Membership Manager Pro Cross-Site Scripting and SQL Injection Vulnerability
  - Rebrand P2P Share Spy Information Disclosure Vulnerability
  - Runtime GetDataBack for NTFS Local Information Disclosure Vulnerability
- UNIX / Linux Operating Systems
  - FreeBSD PortUpgrade Local Insecure Temporary File Handling
  - FreeBSD Kernel AMD64 Unprivileged Hardware Access
  - GNU Core Utilities Race Condition
  - **GNU Sharutils Multiple Buffer Overflow (Updated)**
  - **GNU Sharutils 'Unshar' Insecure Temporary File Creation (Updated)**
  - **Grip CDDB Query Buffer Overflow (Updated)**
  - GwenView Multiple Image Handling Heap-Based Vulnerabilities
  - IBM AIX NIS Client Remote Arbitrary Code Execution
  - **ImageMagick Photoshop Document Buffer Overflow (Updated)**
  - **KDE DCOPServer Local Denial of Service (Updated)**
  - KDE KMail HTML EMail Remote Spoofing
  - Multiple Vendors ImageMagick Multiple Image Handling Heap-Based Vulnerabilities
  - Multiple Vendors KDE 'kimgio' image library Remote Buffer Overflow
  - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
  - **Multiple Vendors MySQL Database Unauthorized GRANT Privilege (Updated)**
  - **Multiple Vendors GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index (Updated)**
  - **Multiple Vendors Linux Kernel Futex Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Local Buffer Overflows & Information Disclosure (Updated)**
  - **Multiple Vendors Linux Kernel Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ActiveWeb Softwares Active Auction House	Multiple input validation vulnerabilities have been reported that could let a remote malicious user inject SQL commands and conduct Cross-Site Scripting attacks. Input validation errors exist in several scripts and the e-mail field in '/activeauctionsuperstore/sendpassword.asp' permits SQL injection. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ActiveWeb Active Auction House SQL Injection and Cross-Site Scripting Vulnerability CAN-2005-1029 CAN-2005-1030	High	Dcrab 's Security Advisory, April 6, 2005
AN HTTP Server 1.42n	A buffer overflow vulnerability has been reported in 'cmdIS.DLL' that could let a local malicious user execute arbitrary code with the privileges of the web service and remote malicious users conduct Cross-Site Scripting attacks. The server also does not properly validate user-supplied URI input before writing the data to the log file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	AN HTTP Server 'cmdIS.DLL' Buffer Overflow Arbitrary Code Execution and Cross-Site Scripting Vulnerability CAN-2005-1086 CAN-2005-1087	High	SIG^2 Vulnerability Research Advisory, April 7, 2005
Centrinity FirstClass Bookmark 8.0 client	A vulnerability has been reported that could let a remote malicious user execute arbitrary files. This is because a field in the FirstClass bookmark management window is not properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Centrinity FirstClass Bookmark Input File Execution Vulnerability CAN-2005-1045	High	Security Tracker Alert,1013665, April 8, 2005
Computer Associates eTrust Intrusion Detection 3.0	A buffer overflow vulnerability has been reported that could let a remote malicious user cause a Denial of Service. This is because the software does not properly validate user-supplied input provided to the Microsoft Crypto API CPImportKey() function. Update for eTrust Intrusion Detection 3.0: http://supportconnectw.ca.com/premium/etrust/etrust_intrusion/downloads/eid-solpatch_r30.asp#rel30 Update for eTrust Intrusion Detection 3.0 SP1: http://supportconnectw.ca.com/premium/etrust/etrust_intrusion/downloads/eid-solpatch_r30.asp#rel30sp1 Currently we are not aware of any exploits for this vulnerability.	Computer Associates eTrust Intrusion Detection Denial of Service Vulnerability CAN-2005-0968	Low	iDEFENSE Security Advisory 04.05.05
DameWare Development DameWare Mini Remote Control 3.x prior to 3.80; 4.x prior to 4.9	A vulnerability has been reported that could let a remote authenticated malicious user gain elevated privileges. Fixed versions (3.80, 4.9) are available: http://www.dameware.com/support/security/bulletin.asp?ID=SB5 Currently we are not aware of any exploits for this vulnerability.	DameWare Mini Remote Control Privilege Escalation Vulnerability CAN-2005-1088	Medium	DameWare Security Bulletin #: 5, April 5, 2005
GNU DC++ prior to 0.674	A vulnerability has been reported that could let malicious users append data to arbitrary files. Update to version 0.674: http://dcplusplus.sourceforge.net/index.php?t=2&s=1 Currently we are not aware of any exploits for this vulnerability.	GNU DC++ Arbitrary Files Modification Vulnerability CAN-2005-1089	Medium	DC++ News: Security fix April 11, 2005

GNU Maxthon (MyIE2) 1.2.0 and 1.2.1	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. This is because the security ID of a plug-in is not properly protected from being included and accessed on an external website via the script tag. Update to version 1.2.2: http://www.maxthon.com/download.htm A Proof of Concept exploit has been published.	GNU Maxthon Security ID Disclosure Vulnerability CAN-2005-1090 CAN-2005-1091	High	Aviv Raff Security Advisory, April 8, 2005
Lightspeed Technologies DeluxeFTP 6.01	A security issue has been reported that could let a local malicious user view sensitive information. User credentials are stored in plain text in 'sites.xml.' No workaround or patch available at time of publishing. There is no exploit code required.	Lightspeed Technologies DeluxeFTP Information Disclosure Vulnerability CAN-2005-1092	Medium	Security Focus, Bugtraq ID 13105, April 12, 2005
MailEnable MailEnable Enterprise Edition 1.x MailEnable Professional 1.54	A buffer overflow vulnerability has been reported that could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. This is due to a boundary error in the IMAP service when handling the 'LOGIN' command. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	MailEnable IMAP 'LOGIN' Command Buffer Overflow Vulnerability CAN-2005-1015	Low/ High (High if arbitrary code can be executed)	Secunia SA14870, April 7, 2005
Microsoft Exchange 2000 Server SP3, 2003, 2003 SP1	A vulnerability has been reported due to an unchecked buffer in the SMTP service that could let a remote malicious user execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-021.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Exchange Server Remote Code Execution Vulnerability CAN-2005-0560	High	Microsoft Security Bulletin. MS05-021, April 12, 2005 Technical Cyber Security Alert TA05-102A US CERT VU#275193
Microsoft Internet Explorer 5.01, 5.5, 6	Multiple vulnerabilities have been reported that include DHTML Object Memory Corruption, URL Parsing Memory Corruption, and Content Advisor Memory Corruption Vulnerability. These vulnerabilities could let remote malicious users execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-020.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Remote Code Execution Vulnerability CAN-2005-0553 CAN-2005-0554 CAN-2005-0555	High	Microsoft Security Bulletin MS05-020, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#774338, VU#756122, VU#222050
Microsoft Jet Database msjet40.dll library version 4.00.8618.0	A vulnerability was reported that could let a remote malicious user cause arbitrary code to be executed. This is because the 'msjet40.dll' component does not properly validate user-supplied input when parsing database files. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Jet Database Remote Code Execution Vulnerability **CAN-2005-0944** **(Updated CVE)**	High	Hexview Advisory, ID: HEXVIEW*2005*03*31*1
Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx V1.1: Bulletin updated with information on the mandatory upgrade of vulnerable MSN Messenger clients in the caveat section, as well as changes to the Workarounds for PNG Processing Vulnerability in MSN Messenger – CAN-2004-0597 V1.2: Bulletin updated with correct file version information for Windows Messenger 5.0 update, as well as added Windows Messenger 5.1 to "Non-Affected Software" list. **V2.0: The update for Windows Messenger version 4.7.0.2009 (when running on Windows XP Service Pack 1) was failing to install when distributed via SMS or AutoUpdate. An updated package corrects this behavior.** An exploit script has been published for MSN Messenger/Windows Messenger PNG Buffer Overflow vulnerability.	Microsoft Media Player & Windows/MSN Messenger PNG Processing CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890 SecurityFocus, February 10, 2005 Microsoft Security Bulletin MS05-009 V1.1, February 11, 2005 Microsoft Security Bulletin, MS05-009 V1.2, February 15, 2005 **Microsoft Security Bulletin, MS05-009 V2.0, April 12,**

				2005
Microsoft MSN Messenger 6.2	A vulnerability has been reported because MSN Messenger may not process a malformed GIF image with an improper height and width. This could let remote malicious users execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-022.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft MSN Messenger Remote Code Execution Vulnerability CAN-2005-0562	High	Microsoft Security Bulletin MS05-022, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#633446
Microsoft Outlook 2003, XP Outlook Web Access 2003	A vulnerability has been reported that could let a remote malicious user can spoof 'From' addresses. A remote user can send e-mail with a specially crafted 'From' address header line that contains multiple e-mail addresses, the user's client will display only the first address. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Outlook and Outlook Web Access Email Spoofing Vulnerability CAN-2005-1052	Low	iDEFENSE Security Advisory 04.08.05
Microsoft Windows (XP SP2 is not affected)	A Denial of Service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx Bulletin V1.1 (January 20, 2005): Updated CAN reference and added acknowledgment to finder for CAN-2004-1305. V1.2 Frequently Asked Questions updated to reflect Windows 98, 98SE and ME security update availability. **V2.0 Customers deploying the Windows 98, 98SE and ME security update caused machines to unexpectedly restart. Microsoft has made available revised security updates for these platforms.** Another exploit script has been published.	Microsoft Windows ANI File Parsing Errors CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT VU#177584 & VU#697136 Security Focus, January 12, 2005 Technical Cyber Security Alert, TA05-012A, January 12, 2005 Microsoft Security Bulletin, MS05-002, V1.1, January 20, 2005 PacketStorm, January 31, 2005 Microsoft Security Bulletin, MS05-002, V1.2, March 8, 2005 **Microsoft Security Bulletin, MS05-002, V2.0, April 12, 2005**
Microsoft Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, 98 SE, and ME	Multiple vulnerabilities have been reported that include errors in the font, Kernel, Object Management Vulnerability and CSRSS. These are due to input validation and buffer overflow errors. A malicious user could deny service or obtain escalated privileges. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-018.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows Kernel Elevation of Privilege and Denial of Service Vulnerabilities CAN-2005-0060 CAN-2005-0061 CAN-2005-0550 CAN-2005-0551	Low/ Medium (Medium if elevated privileges can be obtained)	Microsoft Security Bulletin MS05-018, April 12, 2005
Microsoft Windows NT Server 4.0 SP6a, Windows NT Server 4.0 Terminal Server Edition SP6a, Windows 2000 Server SP3 & SP4, Windows 2003, Windows 2003 for Itanium-based Systems **Avaya DefinityOne Media Servers; Avaya IP600**	A buffer overflow vulnerability exists in the License Logging service due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx **A Proof of Concept exploit has been published.**	Microsoft Windows License Logging Service Buffer Overflow CAN-2005-0050	Low/ High (High if arbitrary code can be executed)	Microsoft Security Bulletin, MS05-010, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT

Media Servers; Avaya S3400 Message Application Server; Avaya S8100 Media Servers				Vulnerability Note VU#130433 **Security Focus, Bugtraq ID 12481, April 12, 2005**
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP1 Windows XP 64-Bit Edition SP1 Windows 98 and 98 SE	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-017.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Message Queuing Remote Code Execution Vulnerability CAN-2005-0059	High	Microsoft Security Bulletin MS05-017, April 12, 2005
Microsoft Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows XP 64-Bit Edition SP 1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, 98 SE, ME	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. This is because of an error in the process to validate which application should load a file. A remote user can convince the Windows Shell to start the HTML Application Host application when that application would not typically be used to process files. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-016.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Shell Remote Code Execution Vulnerability CAN-2005-0063	High	Microsoft Security Bulletin MS05-016, April 12, 2005 US-CERT VU#673051
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP 1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, Windows 98 SE, and Windows ME	Multiple vulnerabilities have been reported that include IP Validation, ICMP Connection Reset, ICMP Path MTU, TCP Connection Reset, and Spoofed Connection Request. These vulnerabilities could let remote malicious users execute arbitrary code or execute a Denial of Service. Updates available: http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities CAN-2005-0048 CAN-2004-0790 CAN-2004-1060 CAN-2004-0230 CAN-2005-0688	Low/ High (High if arbitrary code can be executed)	Microsoft Security Bulletin MS05-019, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#233754
Microsoft Word 2000, 2002 Works Suite 2001, 2002, 2003, and 2004 Office Word 2003	A buffer overflow vulnerability has been reported that could lead to remote execution of arbitrary code or escalation of privilege. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-023.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities CAN-2004-0963 CAN-2005-0558	High	Microsoft Security Bulletin MS05-023, April 12, 2005 US-CERT VU#442567, VU#752591
Miranda IM 'PopUp Plus' 2.0.3.8 plugin for Miranda Instant Messenger	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code on the target system. The vulnerability can be exploited if the 'Use SmileyAdd Setting' application menu option is enabled. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Miranda IM PopUp Plus Plugin Remote Code Execution Vulnerability CAN-2005-1093	High	sec.org.il Security Advisory, April 6, 2005
Netscape Netscape Browser 7.2 and prior versions	A vulnerability has been reported in the Javascript regex parsing that could let a remote malicious user can obtain portions of browser memory. This is because the browser's javascript does not properly parse lamba list regular expressions. The vulnerability is in 'js/src/jsstr.c' in the find_replen() function. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netscape Browser Information Disclosure Vulnerability	Medium	Security Tracker Alert ID: 1013643, April 5, 2005
Network-Client.com FTP Now 2.6.14	A vulnerability has been reported that could let a local malicious user obtain FTP passwords. This is because the application stores FTP username and password values on the system in plaintext form. No workaround or patch available at time of publishing. There is no exploit code required.	Network-Client.com FTP Now Local Information Disclosure Vulnerability CAN-2005-1094	Medium	Security Tracker Alert ID: 1013657, April 6, 2005

Ocean12 Technologies Ocean12 Membership Manager Pro 1.x	Two vulnerabilities have been reported that could let a remote user conduct Cross-Site Scripting and SQL injection attacks. This is due to input validation errors in the "page" parameter in "main.asp" and the "UserID" parameter in "main.asp." No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ocean12 Membership Manager Pro Cross-Site Scripting and SQL Injection Vulnerability CAN-2005-1095 CAN-2005-1096	High	Secunia SA14864, April 7, 2005
Rebrand Software P2P Share Spy 2.2	A vulnerability has been reported that could let a local malicious user obtain the password because it is stored in the Windows Registry in plaintext form. No workaround or patch available at time of publishing. There is no exploit code required.	Rebrand P2P Share Spy Information Disclosure Vulnerability CAN-2005-1097	Medium	Security Tracker Alert ID: 1013673, April 11 2005
Runtime Software GetDataBack for NTFS 2.31	A vulnerability exists that could let a local malicious user obtain the license key. This is because the software stores the username and license key in the Windows Registry. No workaround or patch available at time of publishing. There is no exploit code required.	Runtime GetDataBack for NTFS Local Information Disclosure Vulnerability CAN-2005-1098	Medium	Security Tracker Alert ID: 1013644, April 5, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
FreeBSD FreeBSD 4.0 .x, 4.0, -RELENG, alpha, 4.1, 4.1.1, -STABLE, -RELEASE, 4.2, -STABLEpre122300, -STABLEpre050201, -STABLE, -RELEASE, 4.3, -STABLE, -RELENG, -RELEASE-p38, -RELEASE, 4.4, -STABLE, -RELENG, -RELEASE-p42, 4.5, -STABLEpre2002-03-07, -STABLE, -RELENG, -RELEASE-p32, -RELEASE, 4.6, -STABLE, -RELENG, -RELEASE-p20, -RELEASE, 4.6.2, 4.7, -STABLE, -RELENG, -RELEASE-p17, -RELEASE, 4.8, -RELENG, -RELEASE-p7, -PRERELEASE, 4.9, -RELENG, -PRERELEASE, 4.10, -RELENG, -RELEASE, 4.11 -STABLE, 5.0, -RELENG, -RELEASE-p14, alpha, 5.1, -RELENG, -RELEASE/Alpha, -RELEASE-p5, -RELEASE, 5.2, -RELENG, -RELEASE, 5.2.1, -RELEASE, -STABLE, -RELENG, 5.3, -RELEASE, 5.4, -RELEASE, -PRERELEASE	A vulnerability has been reported in portupgrade due to a failure to securely handle temporary files, which could let a malicious user corrupt arbitrary files and potentially execute code. Update to version 20041226_2. There is no exploit code required.	FreeBSD PortUpgrade l Insecure Temporary File Handling CAN-2005-0610	High	Security Focus, 13106, April 12, 2005
FreeBSD FreeBSD 5.0, -RELENG,, -RELEASE-p14, alpha, 5.1, -RELENG, -RELEASE/Alpha, -RELEASE-p5, -RELEASE, 5.2, -RELENG, -RELEAS, 5.2.1-RELEASE, 5.3, -RELENG, -RELEASE, 5.4 -PRERELEASE	A vulnerability has been reported due to insufficient hardware access restrictions, which could let a malicious user obtain unauthorized access. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:03/amd64.patch Currently we are not aware of any exploits for this vulnerability.	FreeBSD Kernel AMD64 Unprivileged Hardware Access CAN-2005-1036	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:03, April 6, 2005
GNU Coreutils 5.2.1	A vulnerability has been reported in the 'mkdir,' 'mknod,' and 'mkfifo' utilities due to a race condition, which could let a malicious user obtain sensitive information, corrupt data, and potentially obtain elevated privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GNU Core Utilities Race Condition CAN-2005-1039	Medium	Security Focus, 13053, April 7, 2005

GNU sharutils 4.2, 4.2.1	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml FedoraLegacy: http://download.fedoralegacy.org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** We are not aware of any exploits for these vulnerabilities.	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004 Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005 Ubuntu Security Notice, USN-102-1 March 29, 2005 Fedora Update Notifications, FEDORA-2005-280 & 281, April 1, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005**
GNU sharutils 4.2, 4.2.1	A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-06.xml** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	GNU Sharutils 'Unshar' Insecure Temporary File Creation **CAN-2005-0990**	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005 **Gentoo Linux Security Advisory, GLSA 200504-06, April 6, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005**
Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-304.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-07.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CAN-2005-0706	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005 RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:066, April 3, 2005 **Gentoo Linux Security Advisory, GLSA 200504-07, April 8, 2005** **SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005**
Gwenview Gwenview 1.2	Multiple vulnerabilities have been reported when allocating heap-based memory and the chunk size is derived from them image height, width, and plane values due to insufficient sanity checks, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. Currently, we are not aware of any exploits for these	GwenView Multiple Image Handling Heap-Based Vulnerabilities	Low/ High (High if arbitrary code can be executed)	Security Focus, 13098, April 11, 2005

	vulnerabilities.			
IBM AIX 5.3	A vulnerability has been reported in the NIS client which could let a remote malicious user execute arbitrary code with root privileges. Hotfix available at: ftp://aix.software.ibm.com/aix/efixes/security/nis_2_efix.tar.Z Currently we are not aware of any exploits for this vulnerability.	IBM AIX NIS Client Remote Arbitrary Code Execution CAN-2005-1037	High	Secunia Advisory, SA14856, April 6, 2005
ImageMagick ImageMagick 6.x	A buffer overflow vulnerability exists in 'coders/psd.c' when a specially crafted Photoshop document file is submitted, which could let a remote malicious user execute arbitrary code. Update available at: http://www.imagemagick.org/www/download.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-26.xml Gentoo: http://security.gentoo.org/glsa/glsa-200501-37.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	ImageMagick Photoshop Document Buffer Overflow CVE Name: CAN-2005-0005	High	iDEFENSE Security Advisory, January 17, 2005 Ubuntu Security Notice, USN-62-1, January 18, 2005 Debian Security Advisory, DSA 646-1, January 19, 2005 Gentoo Linux Security Advisory, GLSA 200501-26, January 20, 2005 Gentoo Linux Security Advisory, GLSA 200501-37, January 26, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:065, April 3, 2005**
KDE KDE 1.1-1.1.2, 1.2, 2.1-2.1.2, 2.2-2.2.2, 3.0- 3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2	A Denial of Service vulnerability has been reported in the Desktop Communication Protocol (DCOP) daemon due to an error in the authentication process Upgrade available at: http://www.kde.org/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-22.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-325.html ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-307.html** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this	KDE DCOPServer Local Denial of Service CAN-2005-0396	Low	KDE Security Advisory, March 16, 2005 Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005 RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005 ALTLinux Security Advisory, March 29, 2005 **RedHat Security Advisory, RHSA-2005:307-08, April 6,2005** **SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005**

	vulnerability.			
KDE kmail 1.7.1	A vulnerability has been reported due to insufficient sanitization of HTML email messages, which could let a remote malicious user conduct spoofing attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	KDE KMail HTML EMail Remote Spoofing CAN-2005-0404	Medium	Secunia Advisory, SA14925, April 11, 2005
Multiple Vendors ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3.2-1.2.0, 5.5.4, 5.5.6.0-20030409, 5.5.6, 5.5.7, 6.0, 6.0.1-6.0.8, 6.1-6.1.8, 6.2 .0.7, 6.2.0.4, 6.2	Multiple vulnerabilities have been reported when allocating heap-based memory and the chunk size is derived from them image height, width, and plane values due to insufficient sanity checks, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. No workaround or patch available at time of publishing. Currently, we are not aware of any exploits for these vulnerabilities.	ImageMagick Multiple Image Handling Heap-Based Vulnerabilities	Low/ High (High if arbitrary code can be executed)	Security Focus, 13100, April 11, 2005
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE E. Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi?id=10325&action=view http://bugs.kde.org/attachment.cgi?id=10326&action=view SuSE: ftp://ftp.suse.com/pub/suse/ Denial of Service Proofs of Concept exploits have been published.	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	Low/ High (High if arbitrary code can be executed)	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21.x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.54, 3.23.56, 3.23.58, 3.23.59, 4.0.0-4.0.15, 4.0.18, 4.0.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0, 2.1	A vulnerability exists in the 'GRANT' command due to a failure to ensure sufficient privileges, which could let a malicious user obtain unauthorized access. Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2004-611.html SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/m Fedora: http://download.fedora.redhat.com/pub/	MySQL Database Unauthorized GRANT Privilege CAN-2004-0957	Medium	Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005 **Ubuntu Security Notice, USN-109-1 April 06, 2005**

	fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FedoraLegacy: http://download.fedoralegacy.org/fedora/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/** There is no exploit code required.			
Multiple Vendors GNOME GdkPixbuf 0.22 GTK GTK+ 2.4.14 RedHat Fedora Core3 RedHat Fedora Core2	A remote Denial of Service vulnerability has been reported due to a double free error in the BMP loader. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-344.html http://rhn.redhat.com/errata/RHSA-2005-343.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/ **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service CAN-2005-0891	Low	Fedora Update Notifications, FEDORA-2005-265, 266, 267 & 268, March 30, 2005 RedHat Security Advisories, RHSA-2005:344-03 & RHSA-2005:343-03, April 1 & 4, 2005 Ubuntu Security Notice, USN-108-1 April 05, 2005 **SGI Security Advisory, 20050401-01-U, April 6, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:068 & 069, April 8, 2005**
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005:021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux kernel 2.5.0-2.5.69, 2.6-2.6.11	A Denial of Service vulnerability has been reported in 'kernel/futex.c.' **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Futex Denial of Service CAN-2005-0937	Low	Security Tracker Alert, 1013616, March 31, 2005 **Ubuntu Security Notice, USN-110-1 April 11, 2005**

Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Netfilter Memory Leak Denial of Service CAN-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux kernel 2.6 .10, 2.6-2.6.11	Multiple vulnerabilities exist: a vulnerability exists in the 'radeon' driver due to a race condition, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the 'i2c-viapro' driver, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'locks_read_proc()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in 'drivers/char/n_tty.c' due to a signedness error, which could let a malicious user obtain sensitive information; and potential errors exist in the 'atm_get_addr()' function and the 'reiserfs_copy_from_user_to_file_region()' function. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.11-rc4.bz2 SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Exploit scripts have been published.	Linux Kernel Multiple Local Buffer Overflows & Information Disclosure CAN-2005-0529 CAN-2005-0530 CAN-2005-0531 CAN-2005-0532	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14270, February 15, 2005 Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**

	Fedora: **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Trustix: http://http.trustix.org/pub/trustix/updates SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/ Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1- 2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux kernel 2.6.8 rc1-rc3, 2.6.8, 2.6.11 -rc2-rc4, 2.6.11	A Denial of Service vulnerability has been reported due to an error in the AIO (Asynchronous I/O) support in the "is_hugepage_only_range()" function. No workaround or patch available at time of publishing. **An exploit script has been published.**	Linux Kernel Asynchronous Input/Output Local Denial of Service CAN-2005-0916	Low	Secunia Advisory, SA14718, April 4, 2005
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** An exploit script has been published.	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 Security Focus, 12763, March 22, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 **Fedora Update Notification FEDORA-2005-313, April 11, 2005**
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in the '/sys' file system due to a mismanagement of integer signedness, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code. SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntupool/main/l/linux-source-2.6.8.1/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS_Write_File Local Integer Overflow CAN-2005-0867	Low/ High (High if arbitrary code can be executed)	Security Focus, 13091, April 11, 2005
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-05.xml** There is no exploit code required.	Gaim Jabber File Request Remote Denial of Service CAN-2005-0967	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 **Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005**

Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ **Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml** Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005 -298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005 **Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005**
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html **SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 **SGI Security Advisory, 20050401-01-U, April 6, 2005** **RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005**
Paul Vixie Vixie Cron 4.1	A vulnerability has been reported due to insecure creation of temporary files when crontab is executed with the '-e' option, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Vixie Cron Crontab Information Disclosure CAN-2005-1038	Medium	Security Focus, 13024, April 6, 2005

Pavuk Pavuk 0.9pl28i, 0.928r2, 0.928r1, 0.9pl30b, 0.9 pl28, 0.9.31	Multiple unspecified security vulnerabilities have been reported which may result in boundary condition errors. The impact was not specified. Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=81012&package_id=82863&release_id=313436 Currently we are not aware of any exploits for this vulnerability.	Pavuk Multiple Unspecified Security Vulnerabilities CAN-2005-1035	Not Specified	Secunia Advisory, SA14571, April 5, 2005
PHP Group Debian Slackware Fedora pp 4.3.7 and prior	Updates to fix multiple vulnerabilities with php4 which could allow remote code execution. Debian: Update to Debian GNU/Linux 3.0 alias woody at http://www.debian.org/releases/stable/ Slackware: http://www.slackware.com/security/viewer.php?l=slackware- security&y=2004&m=slackware-security.406480 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ Apple: http://www.apple.com/support/downloads/ Debian: http://security.debian.org/pool/updates/main/p/php3/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** An exploit script has been published.	PHP 'memory_limit' and strip_tags() Remote Vulnerabilities CVE Names: CAN-2004-0594 CAN-2004-0595	High	Secunia, SA12113 and SA12116, July 21, 2004 Debian, Slackware, and Fedora Security Advisories Turbolinux Security Advisory TLSA-2004-23, September 15, 2004 PacketStorm, December 11, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 Debian Security Advisory DSA, 669-1, February 7, 2005 **Slackware Security Advisory, SSA:2005-095-01, April 6, 2005**
phpMyAdmin phpMyAdmin 2.0-2.0.5, 2.1- 2.1.2, 2.2, pre 1&pre2, rc1-rc3, 2.2.2-2.2.6, 2.3.1, 2.3.2, 2.4.0, 2.5.0-2.5.2, 2.5.4-2.5.7, 2.6.0pl1-2.6.0pl3, 2.6.1, pl1&pl3, 2.6.1-rc1	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'convcharset' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.2-rc1.tar.gz?download **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-08.xml** There is no exploit code required; however, a Proof of Concept exploit has been published.	phpMyAdmin 'convcharset' Cross-Site Scripting **CAN-2005-0992**	High	phpMyAdmin Security Announcement, PMASA-2005-3, April 3, 2005 **Gentoo Linux Security Advisory, GLSA 200504-08, April 11, 2005**
rsnapshot filesystem snapshot utility 1.0.10, 1.1-1.1.6, 1.2	A vulnerability has been reported in the 'copy_symlink()' function due to improper modification of ownership settings of symbolic link files, which could let a malicious user obtain elevated privileges. Upgrades available at: http://www.rsnapshot.org/downloads/rsnapshot-1.1.7.tar.gz There is no exploit code required.	RSnapshot File Privilege Elevation CAN-2005-1064	Medium	Security Tracker Alert, 1013674, April 11, 2005
SCO Open Server 5.0.6, 5.0.7	Several buffer overflow vulnerabilities have been reported in the 'auditsh,' 'atcronsh,' and 'termsh' programs when handling the 'HOME' variable, which could let a malicious user execute arbitrary code. Upgrades available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.15 Currently we are not aware of any exploits for these vulnerabilities.	SCO OpenServer Auditsh HOME Environment Variable Buffer Overflow CAN-2005-0351	High	SCO Security Advisory, SCOSA-2005.15, April 7, 2005

SGI IRIX 6.5.22 m	Two vulnerabilities have been reported in 'gr_osview' which could let a malicious user cause a Denial of Service, obtain sensitive information, or modify system/user information. Patches available at: ftp://patches.sgi.com/support/free/security/advisories/20050402-01-P.asc There is no exploit code required; however, a Proof of Concept exploit has been published.	SGI IRIX GR_OSView Vulnerabilities CAN-2005-0464 CAN-2005-0465	Low/ Medium (Medium if sensitive information can be obtained or system/user information modified)	SGI Security Advisory, 20050402-01-P, April 7, 2005
SuSE Linux 1.0, 2.0, 3.0, 4.0, 4.2, 4.3, 4.4, 4.4.1, 5.0-5.3, 6.0-6.4, 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386, 7.3, sparc, ppc, i386, 8.0, i386, 8.1, 8.2, 9.0 x86_64 S.u.S.E. Linux 9.0, 9.1, x86_64, 9.2, x86_64	A symbolic link vulnerability has been reported in Texex, which could let a malicious user obtain sensitive information. Upgrades available at: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	SUSE Tetex tmp File Existence Disclosure CAN-2005-1065	Medium	SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005
SuSE Novell Linux Desktop 9.0	A vulnerability has been reported in Netapplet due to insufficient input validation of user-supplied input to network scripts, which could let a malicious user obtain root privileges. Updates available at: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SUSE Netapplet Root Privileges CAN-2005-1040	High	SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005
University of Washington Pine 4.0.2, 4.0.4, 4.2 x, 4.10, 4.20, 4.21, 4.30, 4.33, 4.44, 4.50, 4.52, 4.53, 4.56, 4.58, 4.62	A vulnerability has been reported in 'rpdump' due to a race condition, which could let a malicious user potentially replace a file with a hardlink to a target file No workaround or patch available at time of publishing. There is no exploit code required.	Pine RPDump Local File Corruption CAN-2005-1066	Medium	Security Focus, 13093, April 11, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Access_user Class Access_user Class 1.6	A vulnerability has been reported because the application retains 'new' as a valid password, which could let a remote malicious user obtain unauthorized access. Upgrade available at: http://www.finalwebsites.com/classes/download.php?fc=10 There is no exploit code required.	Access_User Class Arbitrary Account Access CAN-2005-1067	Medium	Secunia Advisory, SA14897, April 8, 2005
AEwebworks Dating Software aeDating 3.2	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'index.php' due to insufficient verification of input passed to the 'skin' parameter, which could let a malicious user include arbitrary files; a vulnerability has been reported in 'sdating.php' due to insufficient sanitization of input passed to the 'event' parameter, which could let a malicious user inject arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported in the control panel due to insufficient sanitization of certain input, which could let a malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	AEwebworks Dating Software Multiple Vulnerabilities CAN-2005-1083 CAN-2005-1084 CAN-2005-1085	High	Secunia Advisory, SA14913, April 12, 2005
Axel Axel 1.0 a	A buffer overflow vulnerability has been reported when handling HTTP redirection, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://wilmer.gaast.net/downloads/axel-1.0b.tar.gz Currently we are not aware of any exploits for this vulnerability.	Axel HTTP Redirection Buffer Overflow CAN-2005-0390	High	Secunia Advisory, SA14831, April 7, 2005

Azerbaijan Development Group AzDGDatingPlatinum 1.1 .0	Multiple vulnerabilities have been reported: SQL injection vulnerabilities have been reported which could let a remote malicious user inject arbitrary SQL code; and Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Azerbaijan Development Group AzDGDating Platinum Multiple Vulnerabilities CAN-2005-1081 CAN-2005-1082	High	Security Focus, 13082, April 9, 2005
brooky.com CubeCart 2.0.0-2.0.6	Vulnerabilities have been reported in the 'index.php,' 'tellafriend.php,' 'view_cart.php,' and 'view_product.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	CubeCart Multiple SQL Injection	High	Security Focus, 13050, April 6, 2005
brooky.com CubeCart 2.x	A vulnerability has been reported in 'index.php' due to insufficient verification of the 'language' parameter, which could let a remote malicious user obtain sensitive information. Update available at: http://www.cubecart.com/site/forums/index.php?act=Downloads Proofs of Concept exploits have been published.	CubeCart Information Disclosure CAN-2005-1033	Medium	Security Tracker Alert, 1013660, April 7, 2005
Cisco Systems IOS 12.x, R12.x	Two vulnerabilities have been reported; a vulnerability has been reported due to an error when processing IKE (Internet Key Exchange) XAUTH messages, which could let a remote malicious user obtain unauthorized access; and a vulnerability has been reported when handling ISAKMP profile attributes, which could let a remote malicious user obtain unauthorized access. Patches available at: http://www.cisco.com/warp/public...sa-20050406-xauth.shtml#software Currently we are not aware of any exploits for these vulnerabilities.	Cisco IOS XAUTH Authentication Bypass CAN-2005-1057 CAN-2005-1058	Medium	Cisco Security Advisory, cisco-sa-20050406, April 6, 2005
Cisco Systems IOS 12.x, R12.x	Two vulnerabilities have been reported: a Denial of Service vulnerability has been reported when the device is configured to employ SSHv2 for remote management and Terminal Access Controller Access Control System Authentication (TACACS+); and a Denial of Service vulnerability has been reported due to a memory leak when authenticating SSH users against a TACACS+ server. Upgrades available at: http://www.cisco.com/warp/public...o-sa-20050406-ssh.shtml#software There is no exploit code required.	Cisco IOS Secure Shell Server Denials of Service CAN-2005-1020 CAN-2005-1021	Low	Cisco Security Advisory, 64439, April 6, 2005
Computer Associates BrightStor ARCServe Backup for Windows 9.0.1, 11.0, 11.1, 11.1 (All), (Client) 11.1, (Eng-All) 9.01, (Eng-Cli) 9.01, (NoEng-All) 9.01, (NoEng-Cli) 9.01, 64 bit 9.0.1, 64 bit 11.0, 64 bit 11.1, BrightStor Enterprise Backup 10.0, 10.5, BrightStor Enterprise Backup for Windows 64 bit 10.5	A buffer overflow vulnerability has been reported in the 'option' field due to a boundary error when receiving certain agent requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available at: http://supportconnect.ca.com/sc/solcenter/ Currently we are not aware of any exploits for this vulnerability.	Computer Associates BrightStor ARCserve Backup UniversalAgent Remote Buffer Overflow CAN-2005-1018	Low/ High (High if arbitrary code can be executed)	iDEFENSE Security Advisory, April 11, 2005
DLMan Pro DLMan Pro 0.9.8	A vulnerability has been reported in the DLMan Pro mod for phpBB due to insufficient sanitization of user-supplied input before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://www.snailsource.com/forum/dlman.php?sid=&func=select_folder&folder_id=15 There is no exploit code required; however, a Proof of Concept exploit has been published.	DLMan Pro Module SQL Injection CAN-2005-1026	High	Security Focus, 13028, April 7, 2005
Elton Muuga sCssBoard 1.0, 1.1, 1.11	Several vulnerabilities have been reported: a vulnerability has been reported because input passed to '[url]' tags may contain JavaScript links, which could let a remote malicious user inject arbitrary script code; and an unspecified error has been reported in the 'profile' page. Upgrades available at:	SCSSBoard URL Tag Script Injection CAN-2005-1068 CAN-2005-1069	High	Secunia Advisory, SA14694, April 7, 2005

	http://prdownloads.sourceforge.net/scssboard/scssboard-1.12.zip?download There is no exploit code required.			
Francisco Burzi PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 FINAL, BETA 1, 6.6, 6.7, 6.9, 7.0 FINAL, 7.0-7.3, 7.6	Cross-Site Scripting vulnerabilities has been reported in the 'Your_Account' module due to insufficient sanitization of the 'username' and 'Avatarcategory' parameters, in the 'Downloads' module, and in 'Banners.PHP,' which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability has been reported in the 'Top' module due to insufficient sanitization of user-supplied input, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP-Nuke Multiple Cross-Site Scripting & SQL Injection CAN-2005-0999 CAN-2005-1027	High	SecurityReason Advisory, April 5, 2005
Francisco Burzi PHP-Nuke 7.6	A vulnerability has been reported in the 'Web_Links' and 'Downloads' modules due to insufficient sanitization of user-supplied input, which could let a remote malicious ser inject arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHP-Nuke SQL Injections CAN-2005-0996 CAN-2005-0997	High	SECURITY REASON.COM Advisory, April 3, 2005
Hewlett Packard Company OpenView Network Node Manager 6.2, Solaris, NT 4.X/Windows 2000, HP-UX 11.X, 6., Solaris, NT 4.X/Windows 2000, HP-UX 11.X, 6.31, Solaris, NT 4.X/Windows 2000, HP-UX 11.X, 7.0 1, Windows 2000/XP, Solaris, HP-UX 11.X, 7.50, Windows 2000/XP, Solaris, Linux, 7.50 HP-UX 11.X	An unspecified remote Denial of Service vulnerability has been reported. Upgrades available at: http://www.itrc.hp.com Currently we are not aware of any exploits for this vulnerability.	HP OpenView Network Node Manager Remote Denial of Service CAN-2005-1056	Low	HP Security Advisory, HPSBMA01125, April 6, 2005
Invision Power Services Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3, Final, 1.3.1 Final	A vulnerability has been reported in the 'st' parameter due to insufficient filter of user-supplied data, which could let a malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board 'ST' Parameter SQL Injection CAN-2005-1070	High	Security Focus, 13097, April 11, 2005
JPortal Web Portal 2.3.1	A vulnerability has been reported in the 'haslo' variable due to insufficient sanitization of user-supplied input passed to the 'module/banner.inc.php' module, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	JPortal Banner.PHP SQL Injection CAN-2005-1071	High	Secunia Advisory, SA14919, April 12, 2005
Lighthouse Development Squirrelcart	A vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'crn' and 'rn' parameters, which could let a remote malicious user execute arbitrary SQL code. **Please contact the vendor to obtain a patch or upgrade.** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Lighthouse Development Squirrelcart SQL Injection CAN-2005-0962	High	Dcrab 's Security Advisory, March 30, 2005 **Security Focus, 12944, April 6, 2005**
Linksys WET11 Wireless Ethernet Bridge, 1.4.3, 1.5.4	A vulnerability has been reported when processing password change requests due to insufficient validation of authentication credentials, which could let a remote malicious user bypass certain security restrictions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Linksys WET11 Password Update Remote Authentication Bypass CAN-2005-1059	Medium	Secunia Advisory, SA14871, April 7, 2005

Linkz Pro Linkz Pro 1.0.3 beta2	A vulnerability has been reported in the Linkz Pro mod for phpBB due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. Patch available at: | http://www.snailsource.com/forum/dlman.php?sid=&func=select_folder&folder_id=13 There is no exploit code required; however, a Proof of Concept exploit has been published.	Linkz Pro Module SQL Injection CAN-2005-1026	High	Security Focus, 13030, April 7, 2005
Macromedia ColdFusion Server MX 6.1	A vulnerability has been reported due to an error in the MX 6.1 updater, which could let a malicious user obtain sensitive information. Workaround available at: http://www.macromedia.com/devnet/security/security_zone/mpsb05-02.html There is no exploit code required.	Macromedia ColdFusion MX Updater Remote Information Disclosure CAN-2005-1022	Medium	Macromedia Security Bulletin, MPSB05-02, April 7, 2005
Meilad File Upload Script 1.1	A vulnerability has been reported in the 'up.php' script due to insufficient restriction of file contents and filename extensions, which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. There is no exploit code required	Meilad File Upload Script PHPBB Module Arbitrary Code Execution CAN-2005-1047	High	Security Tracker Alert, 1013671, April 9, 2005
ModernGigabyte, LLC ModernBill 4.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in 'orderwiz.php' due to insufficient sanitization of the 'c_code' and 'aid' parameters, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported in 'news.php' due to insufficient verification of the 'DIR' parameter, which could let a remote malicious user include arbitrary files. Update available at: http://support.modernbill.com/ There is no exploit code required; however, Proofs of Concept exploits have been published.	ModernGigabyte ModernBill Cross-Site Scripting & File Include CAN-2005-1053 CAN-2005-1054	High	GulfTech Security Research Advisory, April 10th, 2005
Multiple Vendors E-Xoops 1.0 5r3; RunCMS 1.1 A, 1.1	A vulnerability has been reported in the file upload function if the 'Allow custom avatar upload' is enabled due to an input validation error, which could let a malicious user upload arbitrary files. RunCMS: http://www.runcms.org/public/modules/mydownloads/singlefile.php?lid=219 There is no exploit code required.	RunCMS Remote Arbitrary File Upload CAN-2005-1031	High	Secunia Advisory, SA14869, April 7, 2005

Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-04.xml** **SGI:**	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 **Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005** **SGI Security Advisory, 20050401-01-U, April 6, 2005** **Sun(sm) Alert Notification, 57761, April 7, 2005** **SCO Security Advisory, SCOSA-2005.21, April 8, 2005**

	ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21** **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1** **Openwall:** **http://www.openwall.com/Owl/CHANGES-current.shtml** Currently we are not aware of any exploits for these vulnerabilities.			
NetWin SurgeFTP 2.2 m1, 2.2 k3	A remote Denial of Service vulnerability has been reported when the LEAK command is issued to the FTP server. Updates available at: http://netwinsite.com/cgi-bin/keycgi.exe?cmd=download&product=surgeftp There is no exploit code required.	SurgeFTP LEAK Command Remote Denial of Service CAN-2005-1034	Low	SIG^2 Vulnerability Research Advisory, April 7, 2005
Novell Netware 6.0, SP1-SP3, 6.5, SP1.1(b), SP1.1(a), SP1-SP3	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional network traffic in the TCP stack. Patches available at: http://support.novell.com/servlet/filedownload/sec/pub/tcp610jb.exe Currently we are not aware of any exploits for this vulnerability.	Novell NetWare TCP Stack Remote Denial of Service CAN-2005-1060	Low	Novell Technical Information Documents, TID2970467, April 8, 2005
PHP Group PHP prior to 5.0.4	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1 April 05, 2005 **Slackware Security Advisory, SSA:2005-095-01, April 6, 2005**
PostNuke Development Team PostNuke Phoenix 0.760 RC3	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'module' parameter in 'admin.php' and the 'op' parameter in 'user.php,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported due to insufficient sanitization of the 'sid' parameter before used in a SQL query, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PostNuke Phoenix Remote Cross-Site Scripting & SQL Injection CAN-2005-1048 CAN-2005-1049	High	Dcrab 's Security Advisory, April 8, 2005
PunBB PunBB 1.0, RC1&RC2, beta1-beta3, alpha, 1.0.1, 1.1-1.1.5, 1.2.1-1.2.4	Two vulnerabilities have been reported: a vulnerability was reported in the 'profile.php' script due to insufficient sanitization, which could let a remote malicious user obtain administrative access; and a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization os user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PunBB SQL Injection & Cross-Site Scripting CAN-2005-1051 CAN-2005-1072	High	Secunia Advisory, SA14882, April 8, 2005
Qualiteam Corp. LiteCommerce	Multiple SQL injection vulnerabilities have been reported: an input validation vulnerability has been reported in 'cart.php' due to insufficient validation of the 'category_id' and 'product_id' parameters, which could let a remote malicious user inject arbitrary SQL commands; and a vulnerability has been reported when a remote malicious user submits a specially crafted 'target' parameter value, which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	LiteCommerce Multiple SQL Injection Vulnerabilities CAN-2005-1032	Medium/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013658, April 6, 2005

RadScripts RadBids Gold v2	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of some user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'mode' parameter, which could let a remote malicious user inject arbitrary SQL code; and a Directory Traversal vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'read' parameter before used to read files, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	RadScripts RadBids Gold Multiple Vulnerabilities CAN-2005-1073 CAN-2005-1074 CAN-2005-1075	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14906, April 11, 2005
smarty.php.net prior to 2.6.8	A vulnerability has been reported in 'libs/plugins/modifier.regex_replace.php' due to insufficient validation of the 'search' parameter, which could let a malicious user execute PHP code. Update available at: http://smarty.php.net/download.php **Gentoo: http://security.gentoo.org/glsa/glsa-200503-35.xml** Currently we are not aware of any exploits for this vulnerability.	Smarty 'regex_replace' Modifier Template Arbitrary PHP Code Execution CAN-2005-0913	High	Security Tracker Alert, 1013556, March 24, 2005 **Gentoo Linux Security Advisory [UPDATE], GLSA 200503-35:02, April 11, 2005**
Sun Microsystems, Inc. Java 2 Standard Edition SDK 1.4.2, 1.5	A Directory Traversal vulnerability has been reported in the Java Archive Tool, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Sun J2SE Software Development Kit Java Archive Tool Directory Traversal CAN-2005-1080	Medium	Securiteam, April 11, 2005
Sun Microsystems, Inc. OpenOffice 1.1.4, 2.0 Beta	A vulnerability has been reported due to a heap overflow when a specially crafted malformed '.doc' file is opened, which could lead to a Denial of Service or execution of arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	OpenOffice Malformed Document Remote Heap Overflow CAN-2005-0941	Low/ High (High if arbitrary code can be executed)	Security Focus, 13092, April 11, 2005
Sybase Adaptive Server Enterprise 11.0.3.3Linux, 11.5 Win, Sun, HP, 11.5.1 Win, Sun, HP, Digital UNIX, 11.9.2 Sun, HP, Digital UNIX, 12.0 Win, Sun, HP, 12.0 .0.8 EDS#3, 12.0.1 Win, Sun, HP, Digital UNIX, 12.5 Win, Sun, SGI, HP, Digital UNIX, 12.5.2, 12.5.3	Buffer overflow vulnerabilities have been reported in 'attrib_valid,' "convert,' 'declare data type,' 'abstract plan' syntax, and the 'install java, which could let a remote malicious user execute arbitrary code; and a Denial of Service vulnerability exists in 'XP_SERVER' due to a failure to properly handle malformed network data. Upgrades available at: http://downloads.sybase.com/ Currently we are not aware of any exploits for these vulnerabilities.	Sybase Adaptive Server Enterprise Multiple Vulnerabilities CAN-2005-0441 CAN-2005-0942	High	NGSSoftware Insight Security Research Advisory, April 5, 2005
tower.hybryd.org TowerBlog 0.2, 0.4 -r1, 0.6 -r1, 0.6	A vulnerability has been reported in '_dat/login' because user credentials are stored inside the web root, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	TowerBlog Information Exposure CAN-2005-1055	Medium	Securiteam, April 11, 2005
WebCT WebCT Campus Edition 4.1	A vulnerability has been reported due to insufficient sanitization of user-supplied input before used in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WebCT Discussion Board Arbitrary Code Execution CAN-2005-1076	High	Security Focus, 13101, April 11, 2005
XAMPP Apache Distribution 1.4.1-1.4.13, Apache Distribution for Solaris 0.1-0.3	Vulnerabilities has been reported in 'cds.php, 'Guestbook-EN.PL,' 'Phonebook.PHP' due to insufficient sanitization of user-supplied input before included in dynamically generated Web content, which could let a remote malicious user execute arbitrary script code; and a vulnerability has been reported due to a failure to properly secure password access, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	XAMPP Remote HTML Injection & Password Disclosure CAN-2005-1077 CAN-2005-1078	High	Security Focus, 13126, 13127, 13128, 13131, April 12, 2005

zOOm Media Gallery zOOm Media Gallery 2.1.2	A vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	zOOm Media Gallery 'Index.PHP' SQL Injection CAN-2005-1079	High	Securiteam, April 11, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
April 11, 2005	kMailEmailSpoofingPoC.pl	No	Proof of Concept exploit for the KDE KMail HTML EMail Remote Email Content Spoofing vulnerability.
April 8, 2005	punbb_sql.py	No	Exploit for the PunBB 'Profile.PHP' SQL Injection vulnerability.
April 6, 2005	aiodio_read.c	No	Exploit for the Linux Kernel Asynchronous Input/Output Local Denial of Service vulnerability.
April 5, 2005	mailenable_smtpd.pl	Yes	Perl script that exploits the MailEnable SMTP Malformed EHLO Request Denial of Service vulnerability.

[back to top]

Trends

- **Virginia lawmakers aim to hook cyberscammers:** The Virginia General Assembly passed several new bills this year aimed at cracking down on computer and online crimes, including a statute that observers say is the nation's first law that criminalizes "phishing" schemes. Source: http://www.washingtonpost.com/wp-dyn/articles/A40578-2005Apr9.html.
- **Authorities on trail of identity theft rings:** According to law enforcement officials recent investigations of online identity-theft rings show a disturbing pattern. Large groups of criminals are banding together to steal financial data from individuals, and then trade or sell that data on underground Internet sites. Source: http://www.capecodonline.com/cctimes/biz/authoritieson10.htm.
- **IM threats rising sharply, reports confirm:** According to new research in a report issued by the IMlogic Threat Center, IM-borne security threats have increased dramatically in volume since the start of 2005. The quantity of instant messaging threats increased 250 percent in the first quarter of 2005, compared with the same period last year. The research, which tracks viruses, worms, spam and phishing attacks sent over public IM networks, also contends that reported incidents of newly discovered IM threats have grown by 271 percent this year.Source: http://news.com.com/IM+threats+rise+sharply%2C+report+confirms/2100-7349_3-5655267.html.
- **Fighting back against phishing:** Phishing exploits continue to increase at an alarming rate. In the past year, attacks have grown in volume and sophistication, but online merchants are on the offensive with consumer education and new authentication tools. Source: http://www.nwfusion.com/research/2005/041105phish.html?ts
- **Security jargon confuses Internet users**: The average home computer user is confused by technology jargon which is used to warn people about the most serious security threats online. Many are often left vulnerable because they have no idea what they are supposed to be protecting themselves against, a survey for AOL UK has found. For example, eighty-four percent did not know that phishing describes faked e-mail scams. Source: http://news.bbc.co.uk/1/hi/technology/4413155.stm
- **Web postcards hide Trojan horse programs**: SANS Institute's Internet Storm Center (ISC) is warning about e-mail messages that pose as Web postcards, then direct recipients to a Web site that installs a Trojan horse program. The new attacks use sophisticated social engineering techniques to trick users into installing Trojan remote access programs that can fool antivirus and firewall software by appearing to be authorized applications like Internet Relay Chat (IRC) software, the ISC said. Source: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,100874,00.html
- **Antivirus firm warns of Microsoft security Trojan horse**: A new campaign by malicious hackers uses a Web site designed to look like Microsoft's Windows update page to trick Internet users into infecting their computers with a Trojan horse remote-access program, according to antivirus experts at Sophos PLC. The scam uses e-mail messages that appear to come from Microsoft to get recipients to visit a Web page that uploads the malicious program. Source: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,100954,00.html?from=story%5Frules

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Stable	March 2004
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Mytob.C	Win32 Worm	New to Table	March 2005
5	Bagle.BJ	Win32 Worm	Decrease	January 2005
6	Netsky-D	Win32 Worm	Stable	March 2004
6	Netsky-Z	Win32 Worm	Increase	April 2004
7	Zafi-B	Win32 Worm	Decrease	June 2004
7	Netsky-B	Win32 Worm	Stable	February 2004
8	Bagle-AU	Win32 Worm	Increase	October 2004
8	Sober-I	Win32 Worm	Increase	November 2004

Table Updated April 12, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Crowt.D**: A new variant of the Crowt worm blocks an infected user's browser from accessing certain antivirus vendors' Web sites. The virus is noteworthy because it has the potential to send a victim to a phishing Web site even when they have manually typed in a Web address, which is especially dangerous when using an online banking service. Source: http://www.zdnet.com.au/news/security/0,2000061744,39187608,00.htm
- **Fontal.A**: This Trojan, reported by F-Secure, affects Nokia Series 60 handsets running the Symbian operating system and can cause the phone to crash. Fontal.A tries to install a corrupted file, called "Kill Saddam By OID500.sis," into the infected device, causing it to fail at the next reboot. F-Secure did not say whether any infections had been reported. Source: http://news.com.com/Trojan+horse+takes+down+smart+phones/2100-7349_3-5657724.html?tag=nefd.top

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Verify		Trojan
Fontal.A	SymbOS.Fontal.A SymbOS/Fontal.A SYMBOS_FONTAL.A	Symbian OS Virus
Kelvir.f	IM-Worm.Win32.Kelvir.f	Win32 Worm
Mytob.gen	W32/Mytob.gen.worm	Win32 Worm
PWS-Banker.q		Trojan
PWSteal.Cardwiz		Trojan
PWSteal.Ldpinch.F		Trojan
Troj/Ablank-P	Trojan.Win32.StartPage.uz Trojan.Startpage-227	Trojan
Troj/Agent-DH	BackDoor-COC Trojan.Win32.Dialer.gq	Trojan
Troj/Istsvc-A		Trojan
Troj/Nuclear-F	Backdoor.Win32.Nuclear.b	Trojan
Troj/Shed-A	Trojan-Clicker.Win32.Small.fb	Trojan
TROJ_BANKER.MW	PWSteal.Bancos.gen	Trojan
TROJ_IMABUT.A		Trojan
TROJ_MITGLIDER.L		Win32 Worm
Trojan.Anicmoo.D		Trojan
Trojan.SpBot		Trojan
Trojan.Webus.E		Trojan
VBS.Ypsan.D@mm		Visual Basic Virus
W32.Dreffort		Win32 Worm
W32.Kelvir.K	W32/Kelvir.G Win32.Bropia.Z Worm:Win32/Kelvir.J WORM_KELVIR.K	Win32 Worm
W32.Kelvir.O		Win32 Worm
W32.Kelvir.Q		Win32 Worm
W32.Kipis.N@mm		Win32 Worm
W32.Myfip.AB		Win32 Worm
W32.Randex.DFJ		Win32 Worm
W32.Spybot.LXJ		Win32 Worm

W32.Spybot.LZI		Win32 Worm
W32.Spybot.NLI		Win32 Worm
W32/Agobot-RJ		Win32 Worm
W32/Kelvir-H		Win32 Worm
W32/MyDoom-AJ		Win32 Worm
W32/Mytob-AB		Win32 Worm
W32/Mytob-S		Win32 Worm
W32/Mytob-W	Net-Worm.Win32.Mytob.q WORM_MYTOB.W	Win32 Worm
W32/Rbot-AAC		Win32 Worm
W32/Rbot-AAF	Backdoor.Win32.Rbot.nf WORM_RBOT.BBP	Win32 Worm
W32/Rbot-AAG	W32/Sdbot.worm.gen.g W32.Spybot.Worm WORM_SDBOT.ANJ	Win32 Worm
W32/Rbot-AAJ	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Reper-A	Virus.Win32.Repka.a W32/Sautor.worm.gen W32.Reper.A WORM_REPER.A	Win32 Worm
W32/Sdranck-C	WORM_SDBOT.DTR	Win32 Worm
W32/Tirbot-D		Win32 Worm
W97M.Spatch		MS Word Virus
Win32.Abnact.A		Win32 Worm
Win32.Canbede		Win32 Worm
Win32.Dyfuca		Win32 Worm
Win32.Looked.B		Win32 Worm
Win32.SillyDl.KI		Win32 Worm
Win32.Winshow.BD		Win32 Worm
WM97/Xaler-A	Virus.MSWord.Xaler.a W97M.Lexar.A	MS Word Virus
WORM_APRIFUL.A	W32.Aprilcone.A@mm	Win32 Worm
WORM_CROWT.D		Win32 Worm
WORM_KELVIR.L	W32/Kelvir-H Win32.Bropia.AB Worm:Win32/Kelvir.L	Win32 Worm
WORM_MITGLEID.B		Win32 Worm
WORM_MYDOOM.AJ	W32.Mydoom.AU@mm W32/Mydoom.BD@mm Win32/Mydoom.AO@mm	Win32 Worm
WORM_MYFIP.R	W32.Myfip.AB W32/Myfip-L	Win32 Worm
WORM_MYTOB.AA	W32.Mytob.U@mm W32/Mytob.AG@mm	Win32 Worm
WORM_MYTOB.AB	W32.Mytob.AD@mm W32/Mytob-S W32/Mytob.AH@mm	Win32 Worm
WORM_MYTOB.AC	W32.Mytob.AG@mm W32/MyDoom-AJ W32/Mytob.AJ@mm Win32.Mytob.AE Win32/Mytob.Q@mm	Win32 Worm
WORM_MYTOB.AD	W32.Mytob.AH@mm W32/Mytob-E W32/Mytob.AL@mm Win32.Mytob.AF Win32/Mytob.W@mm	Win32 Worm
WORM_MYTOB.AE	W32.Mytob.AI@mm W32/Mytob-E	Win32 Worm
WORM_MYTOB.AF	W32/Mytob-AA W32/Mytob.AM@mm Win32.Mytob.AD Win32/Mytob.X@mm	Win32 Worm
WORM_MYTOB.AG	W32/Mytob.AO@mm Win32/Mytob.Y@mm	Win32 Worm
WORM_MYTOB.AH	W32/Mytob-X W32/Mytob.AP@mm	Win32 Worm
WORM_MYTOB.AI	W32/Mytob-Y W32/Mytob.AN@mm	Win32 Worm

WORM_MYTOB.AK	W32.Mytob.AK@mm W32/Mytob-Z	Win32 Worm
WORM_MYTOB.AL	W32.Mytob.AL@mm	Win32 Worm
WORM_MYTOB.AM	W32.Mytob.AM@mm W32/Mytob-AB	Win32 Worm
WORM_MYTOB.AM	W32.Mytob.AM@mm W32/Mytob-AB	Win32 Worm
WORM_MYTOB.AN	W32.Mytob.AE@mm W32.Mytob.AN@mm W32/Mytob-E Win32.Mytob.AC	Win32 Worm
WORM_MYTOB.AO	W32.Mytob.AO@mm	Win32 Worm
WORM_MYTOB.AP	WORM_MYTOB.AP	Win32 Worm
WORM_MYTOB.AU		Win32 Worm
WORM_MYTOB.AV	W32/Mytob-AV	Win32 Worm
WORM_MYTOB.AX		Win32 Worm
WORM_MYTOB.BA		Win32 Worm
WORM_PREX.A	W32.Kelvir.O W32/Bropia-L Win32.Bropia.AA	Win32 Worm
WORM_VERFUN.A	Backdoor.Verify Backdoor:Win32/Verify.B Win32.Verify.B	Win32 Worm
X97M.Yini		Word 97 Virus

[back to top]

Last updated April 13, 2005